Une idée à un million de ~~dollars~~problèmes ?

Laurent Lyaudet*

15 juillet 2025

Version initiale : 2025/07/15 Version courante : 2025/07/15
Mots-clés : one-way function, random noise XD

— Arrête avec les titres ronflants !

— Si je veux ! XD

Dans cette note, je vais parler d'une idée amusante que j'ai eue pendant ma thèse (j'ai dû en parler dans notre bureau de thésards) : et s'il y avait des "one-way functions" qui ne peuvent sécuriser que du bruit aléatoire ? Si c'était le cas de RSA ? Eh oui, car les messages humains sont très loins du bruit aléatoire. Ils ont une entropie faible. Donc ce serait amusant que certaines one-way functions soient cassables facilement si on les utilise pour transmettre des informations d'entropie faible. Ce seraient des one-way functions qui ne sont bonnes que pour le bruit aléatoire : des "random noise one-way functions". Alors, tu vas me dire : ≪ Compresse ton message, il aura une forte entropie, et c'est gagné. ≫. Mais je vais te répondre : mon professeur de codage/théorie de l'information en maîtrise informatique nous expliquait qu'il y a des algorithmes de compression quasi-optimaux selon la théorie de l'information ; le quasi étant lié à la table de correspondance qui ajoute un "overhead" fâcheux. Donc même compressé, il y a cette table et ce n'est toujours pas "random noise". En plus, dans un protocole d'échange à clé publique renforcé (hardened), tu sais où doit se trouver la table dans le clair... Peut-être que c'est une idée à la con, et peut-être pas.

Encore plus fort et encore moins intuitif : et s'il y avait une one-way function qui n'est pas random noise, style RSA, mais qui est vulnérable aux ordinateurs quantiques ; alors qu'il existe une random noise one-way function qui résiste aux ordinateurs quantiques si c'est bien du random noise. Ce serait contre-intuitif mais le monde des mathématiques est parfois surprenant, comme mon résultat d'inversion de complexité dans Lyaudet(2010) (il y a bien d'autres résultats contre-intuitifs).

Et si, a contrario, un clair avec une forte entropie augmentait les chances d'un autre type d'attaque, sortant des signaux radios de la clé de l'algorithme du fond du message, car ça devient la seule partie répétitive.

RSA aura 50 ans dans 2 ans, et c'est toujours utilisé. Pendant ma thèse entre 2004 et 2007, j'étais persuadé que ce serait remplacé dans les 10 ans (au moins par de la cryptographie quantique inviolable pour les communications étatiques). Belle longévité pour un algorithme aussi simple.

L. Lyaudet. NP-hard and linear variants of hypergraph partitioning. *Theor. Comput. Sci.*, 411(1) :10–21, 2010. doi : 10.1016/J.TCS.2009.08.035. URL https://doi.org/10.1016/j.tcs.2009.08.035.

*https://lyaudet.eu/laurent/, laurent.lyaudet@gmail.com